4.50 (a) If \( f \) is any function, 
\[
\sum_{0 \leq k < m} f(k) = \sum_{d \mid m} \sum_{0 \leq k < m} f(k)[d = \gcd(k, m)]
\]
\[
= \sum_{d \mid m} \sum_{0 \leq k < d} f(k)[k \perp \frac{m}{d}]
\]
\[
= \sum_{d \mid m} \sum_{0 \leq k < d} f(kd)[k \perp \frac{m}{d}]
\]
\[
= \sum_{d \mid m} \sum_{0 \leq k < d} f(km/d)[k \perp d]
\]
we saw a special case of this in the derivation of (4.63). An analogous derivation holds for \( \prod \) instead of \( \sum \). Thus we have
\[
z^m - 1 = \prod_{0 \leq k < m} (z - \omega^k) = \prod_{d \mid m} \prod_{0 \leq k < d} (z - \omega^{km/d}) = \prod_{d \mid m} \Psi_d(z)
\]
because \( \omega^{m/d} = e^{\frac{2\pi i}{d}} \).

Part (b) follows from part (a) by the analog of (4.56) for products instead of sums. Incidentally, this formula shows that \( \Psi_m(z) \) has integer coefficients, since \( \Psi_m(z) \) is obtained by multiplying and dividing polynomials whose leading coefficient is 1.

4.51 \((x_1 + \cdots + x_n)^p = \sum_{k_1 + \cdots + k_n = p} \frac{p!}{(k_1! \cdots k_n!)} x_1^{k_1} \cdots x_n^{k_n}, \text{ and the coefficient is divisible by } p \) unless some \( k_i = p \). Hence \((x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \) (mod \( p \)). Now we can set all the \( x \)'s to 1, obtaining \( n^p \equiv n \).

4.52 If \( p > n \) there is nothing to prove. Otherwise \( x_1 \perp p \), so \( x^k(p-1) \equiv 1 \) (mod \( p \)); this means that at least \([n-1]/(p-1)] \) of the given numbers are multiples of \( p \). And \((n-1)/(p-1) \geq n/p \) since \( n \geq p \).

4.53 First show that if \( m \geq 6 \) and \( m \) is not prime then \((m-2)! \equiv 0 \) (mod \( m \)). (If \( m = p^2 \), the product for \((m-2)!\) includes \( p \) and \( 2p \); otherwise it includes \( d \) and \( m/d \) where \( d < m/d \).) Next consider cases:

Case 0, \( n < 5 \). The condition holds for \( n = 1 \) only.

Case 1, \( n \geq 5 \) and \( n \) is prime. Then \((n-1)!/(n+1) \) is an integer and it can’t be a multiple of \( n \).

Case 2, \( n \geq 5 \), \( n \) is composite, and \( n + 1 \) is composite. Then \( n \) and \( n+1 \) divide \([n-1]!\), and \( n \perp n+1 \); hence \( n|[n+1]/[n-1]!\).

Case 3, \( n \geq 5 \), \( n \) is composite, and \( n + 1 \) is prime. Then \((n-1)! \equiv 1 \) (mod \( n + 1 \)) by Wilson’s theorem, and
\[
[n-1]!/[n+1] = ([n-1]+n)/(n+1);
\]